

[NEWS] Apple QuickTime Malformed GIF Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00063.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 17:12:45 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Apple QuickTime Malformed GIF Heap Overflow

SUMMARY

<<http://www.apple.com/quicktime/>> QuickTime is "a multimedia technology developed by Apple Computer, capable of handling various formats of digital video, sound, text, animation, music, and immersive panoramic (and sphere panoramic) images".

eEye Digital Security has discovered a critical heap overflow in the Apple Quicktime player that allows for the execution of arbitrary code via a maliciously crafted GIF file. The flaw has proven to allow for reliable control of data on the heap chunk and can be exploited via a web site by using ActiveX controls.

DETAILS

Vulnerable Systems:

- * Quicktime on Windows 2000
- * Quicktime on Windows XP
- * Quicktime on Mac OS X 10.3.9
- * Apple iTunes on Windows 2000
- * Apple iTunes on Windows XP

[NEWS] Apple QuickTime Malformed GIF Heap Overflow

* Apple iTunes on OS X 10.3.9

When Quicktime processes the Netscape Navigator Application Extension Block of a GIF file, it does not perform proper bounds checking, so it will allocate memory without checking the heap size. The heap can be overwritten in the Picture Modifier block.

The block size calculate code such as:

```
text:66A339CC mov ax, [esi+0Ch]
text:66A339D0 xor ecx, ecx
text:66A339D2 mov [esp+34h+var_28], ecx
text:66A339D6 mov [esp+34h+var_24], ecx
text:66A339DA mov [esp+34h+var_20], ecx
text:66A339DE mov [esp+34h+var_1C], ecx
text:66A339E2 mov word ptr [esp+34h+var_10], cx
text:66A339E7 mov [esp+34h+arg_4], eax
text:66A339EB movsx eax, ax
text:66A339EE mov word ptr [esp+34h+var_10+2], cx
text:66A339F3 mov cx, [esi+8]
text:66A339F7 movsx edx, cx
text:66A339FA sub eax, edx
text:66A339FC movsx edx, word ptr [esi+6]
text:66A33A00 add eax, 3Eh
text:66A33A03 push edi
text:66A33A04 movsx edi, word ptr [esi+0Ah]
text:66A33A08 sar eax, 3
text:66A33A0B lea ebx, [esi+6]
text:66A33A0E and eax, 0FFFFFFFCh
text:66A33A11 sub edi, edx
text:66A33A13 movsx edx, ax
text:66A33A16 mov [esi+4], ax
text:66A33A1A imul edi, edx
```

The allocate code is :

```
text:66A33A68 push edi
text:66A33A69 call sub_668B5B30
```

But when it real process data to this memory, it use real decode data to write this memory but didn't check this heap size. This is segment of the write code function(sub_66AE0A70):

```
text:66AE0B18 movsx edx, word ptr [edi+12h] ; default
text:66AE0B1C imul edx, [edi+0Ch]
text:66AE0B20 mov ecx, [edi+4]
text:66AE0B23 inc word ptr [edi+16h]
text:66AE0B27 mov eax, [esp+arg_0]
text:66AE0B2B add edx, ecx
text:66AE0B2D mov [eax], edx
text:66AE0B2F mov eax, [ebp+10h]
text:66AE0B32 test eax, eax
text:66AE0B34 jz short loc_66AE0B62
text:66AE0B36 mov ax, [ebp+1Ch]
text:66AE0B3A mov edx, [ebp+0Ch]
```

[NEWS] Apple QuickTime Malformed GIF Heap Overflow

```
text:66AE0B3D movzx cx, ah
text:66AE0B41 mov ch, al
text:66AE0B43 mov [edx], cx
text:66AE0B46 movsx eax, word ptr [edi+12h]
text:66AE0B4A imul eax, [ebp+14h]
text:66AE0B4E add eax, [ebp+10h]
text:66AE0B51 mov cx, [ebp+18h]
text:66AE0B55 mov [ebp+0Ch], eax
text:66AE0B58 mov [ebp+1Ah], cx
text:66AE0B5C mov word ptr [ebp+1Ch], 0
```

Vendor Status:

Apple has released a patch for this vulnerability. The patch is available via the Updates section of the affected applications.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2340>>
CVE-2005-2340

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Advisories@xxxxxxxx>> eEye.

The original article can be found at:

<<http://www.eeye.com/html/research/advisories/AD20060111d.html>>
<http://www.eeye.com/html/research/advisories/AD20060111d.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.



- Prev by Date: [\[NEWS\] AmbiCom Bluetooth Object Push Buffer Overflow](#)
- Next by Date: [\[NEWS\] Apple QuickTime QTIF Stack Overflow](#)
- Previous by thread: [\[NEWS\] AmbiCom Bluetooth Object Push Buffer Overflow](#)

[NEWS] Apple QuickTime Malformed GIF Heap Overflow

- Next by thread: [\[NEWS\] Apple QuickTime QTIF Stack Overflow](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)